FORM PTO-1390 (Modified) (REV 11-98) U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

ATTORNEY'S DOCKET NUMBER	U.S. APPLICATION NO. (IF KNOWN, SEE 37 CFR
1236-00	09/701230

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
PCT/US00/26893	29 SEP 00	01 OCT 99

TITLE OF INVENTION
METHOD AND APPARATUS FOR PACKAGING AND TRANSMITTING DATA

APPLICANT(S) FOR DO/EO/US
FRIEDMAN, George; STAREK, Robert Phillip; MURDOCK, Carlos A.

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This is an express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and PCT Articles 22 and 39(1).
4. ☐ A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.
5. ☒ A copy of the International Application as filed (35 U.S.C. 371 (c) (2))
   a. ☐ is transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☐ has been transmitted by the International Bureau.
   c. ☒ is not required, as the application was filed in the United States Receiving Office (RO/US).
6. ☐ A translation of the International Application into English (35 U.S.C. 371(c)(2)).
7. ☐ A copy of the International Search Report (PCT/ISA/210).
8. ☐ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371 (c)(3))
   a. ☐ are transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☐ have been transmitted by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☐ have not been made and will not be made.
9. ☐ A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
10. ☒ An oath or declaration of the inventor(s) (35 U.S.C. 371 (c)(4)).
11. ☐ A copy of the International Preliminary Examination Report (PCT/IPEA/409).
12. ☐ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371 (c)(5)).

Items 13 to 20 below concern document(s) or information included:

13. ☐ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
14. ☒ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
15. ☐ A **FIRST** preliminary amendment.
16. ☐ A **SECOND** or **SUBSEQUENT** preliminary amendment.
17. ☐ A substitute specification.
18. ☐ A change of power of attorney and/or address letter.
19. ☒ Certificate of Mailing by Express Mail
20. ☒ Other items or information:

acknowledgement postcard

505 Rec'd PCT/PTO 28 NOV 2000

U.S. APPLICATION NO. (IF KNOWN, SEE 37 CFR)	INTERNATIONAL APPLICATION NO.	ATTORNEY'S DOCKET NUMBER
09/701230	PCT/US00/26893	1236-00

21. The following fees are submitted:.

BASIC NATIONAL FEE (37 CFR 1.492 (a) (1) - (5)) :

		CALCULATIONS PTO USE ONLY
☐	Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2) paid to USPTO and International Search Report not prepared by the EPO or JPO	**$1,000.00**
☐	International preliminary examination fee (37 CFR 1.482) not paid to USPTO but Internation Search Report prepared by the EPO or JPO	**$860.00**
☒	International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO	**$710.00**
☐	International preliminary examination fee paid to USPTO (37 CFR 1.482) but all claims did not satisfy provisions of PCT Article 33(1)-(4)	**$690.00**
☐	International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(1)-(4)	**$100.00**

ENTER APPROPRIATE BASIC FEE AMOUNT =	**$710.00**	
Surcharge of **$130.00** for furnishing the oath or declaration later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492 (e)).	**$0.00**	

CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE		
Total claims	22 - 20 =	2	x $18.00	**$36.00**	
Independent claims	4 - 3 =	1	x $80.00	**$80.00**	
Multiple Dependent Claims **(check if applicable)**.			☐	**$0.00**	
TOTAL OF ABOVE CALCULATIONS =				**$826.00**	
Reduction of 1/2 for filing by small entity, if applicable. Verified Small Entity Statement must also be filed (Note 37 CFR 1.9, 1.27, 1.28) **(check if applicable)**.			☐	**$0.00**	
SUBTOTAL =				**$826.00**	
Processing fee of **$130.00** for furnishing the English translation later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492 (f)).			+	**$0.00**	
TOTAL NATIONAL FEE =				**$826.00**	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31) **(check if applicable).**			☒	**$40.00**	
TOTAL FEES ENCLOSED =				**$866.00**	
				Amount to be: refunded	$
				charged	$

☒ A check in the amount of **$866.00** to cover the above fees is enclosed.

☐ Please charge my Deposit Account No. in the amount of to cover the above fees.
A duplicate copy of this sheet is enclosed.

☒ The Commissioner is hereby authorized to charge any fees which may be required, or credit any overpayment to Deposit Account No. **13-3405** A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

PAUL A. TAUFER, ESQ.
SCHNADER HARRISON SEGAL & LEWIS, LLP
1600 MARKET STREET, SUITE 3600
PHILADELPHIA, PA 19103
(215) 751-2475
(215) 568-6946 - FAX

SIGNATURE

Paul A. Taufer
NAME

35,703
REGISTRATION NUMBER

November 28, 2000
DATE

METHOD AND APPARATUS FOR PACKAGING AND TRANSMITTING DATA

Field of the Invention

The invention relates to a method and apparatus for packaging and transmitting a file of data. In particular, the invention relates to a method and apparatus for packaging data in a computer executable file, the package having one or more permissions associated with and governing use of the file of data.

Background of the Invention

The 20th century is filled with technological advances, but none more significant than the advent of computers, electronic and digital communications, and the Internet. These technologies have offered the world access to oceans of information on every topic imaginable and have enabled people all over the world to communicate electronically, such as, for example, by sending electronic messages over a network such as the Internet. Cellular and digital technologies have revolutionized the way people communicate via telephone and, in addition, have spawned the development of new devices such as personal digital assistants, pocket personal computers and email pagers that are able to receive and transmit information that can be stored on these devices, forwarded to another device, uploaded onto a computer system, or printed.

A known problem with current technologies is that the author of an electronic message is unable to retain control over what happens to the message after it is transmitted across the network. For example, the recipient may forward the message to another user, print the message, store the message for later viewing, or copy the message to the clipboard. An author may not want a sensitive email or message transmitted to a third party , or a copy of the message stored or printed for future reference. However, current technologies do not completely address this need.

Some email programs allow an author to designate a message as "private." This setting limits a recipients ability to modify an original message and forward it to a third party with the appearance that the message, as modified, was transmitted by the author. However, this setting does not limit a recipient's ability to forward, copy to the clipboard, store or print the message in its original form.

There exists a need in the field of electronic and digital communications to have a method and apparatus that allows an author to set permissions on a communication which restrict the recipient's ability to use the transmitted information. Furthermore, there is also a need for method and apparatus that allows the author to insure that only the intended recipient receives the message. The current invention addresses this need by providing a method and apparatus for generating an encrypted package of data comprising a file of data, a unique identifier, and one or more permissions governing use of the file. The package may also contain the recipient's unique identifier and a client software package to be installed on the recipient's computer system upon receipt of the package.

Summary of the Invention

The invention relates to a method for packaging and transmitting data and a system for carrying out the method. One system of the invention comprises a machine readable medium having information packaging software that generates a computer executable file, a network in communication with the machine readable medium, and a client computer system in communication with the network. A package of information is concatenated into the computer executable file for transmission over the network. In one embodiment, the package of information contains a file of data, a permissions database having one or more permissions associated with the file of data, and encryption software. The client computer is adapted to receive the package of information and execute the computer executable file. The client computer system also has a client permissions database and a vault adapted to receive the package of information.

One method of the invention comprises the steps of receiving a file of data for packaging, receiving a permissions database having one or more permissions associated with the file of data, the one or more permissions governing a client's use of the file, generating a package global unique identifier, generating a package of data comprising the file, the one or more permissions and the global unique identifier, encrypting the package and generating a computer executable file comprising the encrypted package.

Another method of the invention adds to the above-described method the steps of receiving the computer executable file at a client computer system having an operating system and executing the computer executable file at the client computer system. Executing the file comprises the steps of determining whether the operating system is a compatible operating system, and if so, executing a client software on the client computer system. The execution of the client software creates a client permissions database and a vault on the client computer system. After executing the client software, the method further comprises the step of determining whether the encrypted package is valid, and if so, recording the package global unique identifier in the client permissions database, extracting the file of data and the one or more permissions from the package of data, storing the file of data in the vault and storing the one or more permissions in the client permissions database. If the package is not valid, the method sets a state in the computer executable file to indicate that the package is installed.

Brief Description of the Drawings

For the purpose of illustrating the invention, there is shown in the drawings a form which is presently preferred; it being understood, however, that this invention is not limited to the precise arrangements and instrumentalities shown.

Figure 1 is a flow diagram of a system that communicates a package of information according to an embodiment of the invention.

Figure 2 is a flow diagram of a method for communicating an electronic package according to another embodiment of the invention.

Detailed Description of Preferred Embodiments of the Invention

The present invention comprises a novel method and apparatus for packaging data and communicating the package over a network. The terms "computer", "computer system", or "system" as used herein include any device capable of receiving, transmitting, and/or using information, including, without limitation, a processor, a microprocessor, a personal computer, such as a laptop, palm PC, desktop or workstation, a network server, a mainframe, an electronic wired or wireless device, such as for example, a telephone, an interactive television, such as for example, a television adapted to be connected to the Internet or an electronic device adapted for use with a television, a cellular telephone, a personal digital assistant, an electronic pager, and a digital watch. In an illustrative example, information is transmitted in the form of e-mail. A computer, computer system, or system of the invention may operate in communication with other systems over a network, such as, for example, the Internet, an intranet, or an extranet, or may operate as a stand-alone system. Also, the terms "information" and "data" as used herein are each intended to include the broadest definition of the other, and each include text, audio and video data. By way of further example, the term "information"can mean raw data, processed data, or a combination of raw and processed data.

The following description is presented to enable any person skilled in the art to make and use the invention. Descriptions of specific applications are provided only as examples. Various modifications to the preferred embodiment will be readily apparent to those skilled in the art, and the generic principles defined herein may be applied to other embodiments and applications without departing from the spirit and scope of the invention. Thus, the present invention is not intended to be limited to the embodiment shown. On the contrary, the description of the invention set forth herein is intended to cover all alternatives, modifications and equivalents as may be included within the spirit and scope of the invention as defined by the appended claims.

Referring now to Figure 1 there is shown a block diagram of a system that communicates a package of information in accordance with a preferred embodiment of the present invention. A packager 12 generates a computer executable file, such as "package.exe" 14 for transmission over a network 16 to a client computer system 17 for access by a client. The computer executable file 14 comprises a package of information collected by the packager 12.

According to one embodiment of the invention, the package of information includes a file of data 18 and a permissions database 20. In another embodiment of the invention, the package of information further includes encryption software 22 and, optionally but not necessarily, client software 24. Preferably, the client software has a version designation. Packager 12 generates a package global unique identifier (PGUID) for each package of information and includes it in the package of information. In a preferred embodiment, the package of information, including the

PGUID are encrypted by encryption software 22. The PGUID may be, for example, a string of alpha-numeric symbols.

According to a method of the invention, packager 12 receives the file of data 18 and the permissions database 20. The permissions database 20 has one or more author-configurable permissions associated with the file of data 18 that govern use of the file of data 18. One function of these permissions is to restrict sharing of the file of data 18. Exemplary author-configurable permissions include access count, access time, expiration date, authorization date, clipboard permission, print permission, unlimited access permission, application permission, and a system-events permission.

The access account permission specifies the number of times a user may be allowed to access the file of data 18. In an embodiment, one access count is defined as allowing one process on the client computer system 17 to access the file of data 18 for the life of the process. The access time permission specifies the total amount of time in which a client may access a file. Once a process on the client computer system 17 opens the file of data 18, the access time is decremented until the process terminates or, if the access time is completely exhausted before termination of the process, the process is automatically terminated.

The expiration date permission specifies a date on which the file of data will no longer be accessible. A client will have unlimited access to the file, subject to any other permissions on the file of data 18, until the expiration date occurs. If any processes on the client computer system 17 have the file of data 18 open on the expiration date, the processes are automatically terminated. On the expiration date, the file content is overwritten and deleted. Preferably, the expiration date permission is also removed from the permissions data base.

The authorization date permission specifies a date on which the file of data 18 will become accessible. Subject to other permissions on the file of data 18, a user will not be able to access the file of data 18 until that date has passed. All of these access permissions can be configured and enforced independently or in combination.

The clipboard permission specifies whether the client can copy the file of data 18 or a portion of the file, such as, for example, to the Windows clipboard. The clipboard permission may also be configured to prevent the client from forwarding the file of data to another computer system. The print permission specifies whether the client can print the file of data 18. The unlimited access permission grants the client unlimited access to the file of data 18. Preferably, the file of data 18 is read-only, which allows a client with unlimited access permission to view the file of data 18 for an unlimited amount of time. However, the client will not be permitted to do anything more unless other permissions are associated with the file of data 18, such as, for example, print permission, and clipboard permission.

The application permission determines whether one or more of a list of applications is running on the client computer system 17 and disables access to the file of data if one of the

applications is running. Alternatively, the application permission may disable access to the file of data if one of the applications is not running. The system-events permission analyzes the client computer system 17 to determine which system-events have occurred and determines whether to permit access to the file of data 18 based on the system-events that have occurred.

In a preferred embodiment, the packager 12 can define a password to limit access to the package. The package of information will not be accessed until the client enters the appropriate password at the client computer system 17. In another embodiment, the packager 12 may receive a recipient global unique identifier (RGUID) and include it in the package of information. The RGUID identifies the client to whom the author wishes to transmit the file of data 18 and may be manually entered into the package by the author or selected from a list of clients stored in the packager 12.

The package of information is concatenated into the computer executable file 14 for transmission over the network 16 to the client computer system 17.

Referring now to Figure 2, there is shown a method for communicating a package of information after the computer executable file 14 is generated, according to an embodiment of the invention. According to this method, the computer executable file 14, which comprises code to carry out the method, is executed at the client computer system 17, step 30. In the embodiment in which the package is password protected, the client is prompted for the password. In step 32, the client computer system 17 determines whether the operating system is a compatible operating system. If the operating system is not compatible, the package is deleted and overwritten, step 34. Compatible operating systems include but are not limited to Windows 95, 98, NT and 2000. Optionally, as shown in step 36 of Fig. 2, the client computer system 17 determines whether a second package of information is already loaded on the client computer system 17, and if so, terminates the second package, step 38. In step 40, the system 17 determines whether the client software 24 is installed. If the client software is not installed, the client software 24 is extracted from the package and installed on the client computer system 17, step 42. If the client software is installed, the system 17 compares the version of the client software in the package to the version of the software installed, step 44. If the version of the client software in the package is later than the version installed on the system 17, the installed client software is upgraded by extracting the newer version from the package and installing it on the system 17, step 42. In another embodiment, the client software 24 can be extracted from the package and installed without checking for an installed version.

In step 48, the client software 24 is executed creating a client permissions database and a vault on the client computer system. The vault is a virtual disk environment fully integrated with the operating system, yet sequestered from the operating system such that novel operating rules can be implemented and in which files of data can be examined, without risk to the system as a whole. In the embodiment shown in Figure 2, the client software 24 is comprised of one or more device drivers and one or more win32 modules which are installed on the client computer system 17 upon

execution of the software, step 50. At least one of the device drivers or win32 modules creates the client permission database and the vault, step 52. In a preferred embodiment, the win32 module is a modified win32 executable. The device drivers and win32 modules also carry out other functions of the software 24, such as, for example, verifying whether the permissions structure has been altered. Once all the device drivers and win32 modules are loaded, they are cloaked, in part to prevent hacking into the vault, step 54. After the installation of the client software, in a preferred embodiment, the operating system is modified such that the modified win32 executable is automatically initialized when the system 17 is powered-up.

At least one of the device drivers or win32 modules communicates with the computer executable file 14. In one embodiment, one of the win32 modules receives a request to query the package of information, step 56. The win32 module then determines whether the package of information is password protected, step 58, and if so, queries the client for a password, step 60. If the package is not password protected, or it is password protected and the correct password is entered, step 62, then the win32 module determines whether the package is valid, step 64. If the package is valid, the file of data is absorbed into the vault, the one or more permissions are stored in the client permissions database, and the client permissions database is updated with the PGUID, step 66.

Preferably, the validity of a package is determined by reading the PGUID from the package and checking the client permissions database for the PGUID. If the PGUID is in the client permissions database, the package was already received into the vault at another time and the package is invalid. If this occurs, a state in the computer executable file 14 is set to indicate that the package has already been installed. Setting the state may be, for example, changing a data bit or setting a flag. If the PGUID is not in the client permissions database, the package is new to the vault, and is valid.

In the embodiment having a RGUID in the package of information, the validity of a package is determined by checking the client permissions database for the RGUID. If the RGUID in the package of information matches the client's RGUID in the client permissions database, the package is intended for the client receiving the package, and the package is valid. If the RGUID in the package of information does not match the RGUID in the client permissions database, the package is not intended for the client, and the computer executable file 14 is deleted and overwritten, step 68.

After the file of data is absorbed into the vault, the client software 24, preferably via one of the device drivers, deletes and overwrites the computer executable file 14.

In one embodiment, after the package is determined to be valid, but before absorbing the file of data into the vault, the device driver queries the client to create an association to the file of data in the vault. The association is preferably a file, most preferably a "tag" file, which is a substantially zero-byte length file. The client can name the file in a conventional manner. To the client, the file appears to represent the actual file of data in the vault, but it is not. If the client access the properties

of the tag file, a dialog box displays the one or more permissions associated with the file of data.

Once a file name has been chosen and the client has deciphered and transferred the data to the vault, the data is available for access by opening the file of data. This can be done by any user-specified process. If the user double-clicks the file, the application associated with that file-type will automatically start and attempt to open the file via a calling process. The client software 24 intercepts the calling process and performs a security check on the calling process. The security check verifies that the calling process has not created a data hole to "leak" data within the file of data. "Leaking data" means transferring data out of a system in which it is desired to have the data secured. For applications wherein data security is important, there is a need to limit data leakage.

If the calling process passes the security check, a dialog is displayed to the client to verify the client's request for the field of data. The permissions set, comprising one or more permissions, is displayed and any warnings are presented to the client for approval. Warnings include, for example, that all unsaved data will be lost once the field of data is accessed. Once the client agrees, the environment of client computer system 17 changes drastically. No process running of the system 17 will be able to modify anything on the system 17. These restrictions remain in place until the process accessing the file of data quits or is terminated by, for example, an expiration permission.

Claims

What is claimed is:

1. A method for packaging information comprising the steps of:
receiving a file of data for packaging;
receiving a permissions database having one or more permissions associated with the file of data, the one or more permissions governing a client's use of the file;
generating a package global unique identifier;
generating a package of data comprising the file, the one or more permissions and the global unique identifier;
encrypting the package; and
generating a computer executable file comprising the encrypted package.

2. The method of claim 1 wherein the one or more permissions are selected from the group consisting of: an access count permission, an access time permission, an expiration date permission, an authorization date permission, a clipboard permission, a print permission, an unlimited access permission, an application permission, and a system-events permission.

3. The method of claim 1 further comprising the step of setting a password for access to the computer executable file.

4. The method of claim 1 wherein the package of data further comprises a recipient global unique identifier and further comprising the step of receiving the recipient global unique identifier after the step of generating a package global unique identifier.

5. The method of claim 4 wherein the package of data further comprises a client software.

6. A machine-readable medium having a package of information comprising:
a file of data;
a permissions database having one or more permissions associated with the file of data, the one or more permissions governing a client's use of the file;
a package global unique identifier; and
a receiver global unique identifier.

7. The machine readable medium of claim 6 wherein the one or more permissions are selected from the group consisting of: an access count permission, an access time permission, an expiration

date permission, an authorization date permission, a clipboard permission, a print permission, an unlimited access permission, an application permission, and a system-events permission.

8. The machine-readable medium of claim 7 further comprising a client software.

9. A method for communicating a package of information comprising:

receiving a file of data for packaging;

receiving a package permissions database having one or more permissions associated with the file of data, the one or more permissions governing a client's use of the file;

generating a package global unique identifier;

generating a package of data comprising the file of data, the one or more permissions, the global unique identifier, and a client software;

encrypting the package;

generating a computer executable file comprising the encrypted package;

receiving the computer executable file at a client computer system having an operating system;

executing the computer executable file at the client computer system comprising the steps of:

determining whether the operating system is a compatible operating system, and if so,

executing a client software on the client computer system, the execution of the client software creating a client permissions database and a vault on the client computer system; and

determining whether the encrypted package is valid, and if so,

recording the package global unique identifier in the client permissions database,

extracting the file of data and the one or more permissions from the package of data,

storing the file of data in the vault and storing the one or more permissions in the client permissions database,

and if not, setting a state in the computer executable file to indicate that the package is installed.

10. The method of claim 9 further comprising the step of determining whether a second package is loaded on the computer system, and if so, terminating the second package, before the step of executing a client software on the client computer system.

11. The method of claim 9 wherein the step of determining whether the package is valid comprises the steps of searching the client permissions database for the package global unique identifier and, concluding that the package is valid if the package global unique identifier is not in the client permissions database, and concluding that the package is invalid if the package global unique identifier is not in the client permissions database.

12. The method of claim 9 wherein the package further comprises the client software having a version designation and, before the step of executing the client software, determining whether a second version of the client software is installed on the client computer system, and if not, extracting the client software from the package and installing the client software on the client computer system.

13. The method of claim 12 wherein if a second version of the client software is installed on the client computer system, determining whether the version designation of the client software installed on the client computer system is earlier than the second version, and if so, extracting the client software from the package and installing the client software on the client computer system.

14. The method of claim 12 wherein the client software comprises one or more device drivers and the client permissions database and the vault are generated by at least one of the one or more device driver.

15. The method of claim 9 wherein the client software comprises one or more device drivers and the client permissions database and the vault are generated by at least one of the one or more device driver.

16. The method of claim 9 wherein the package further comprises a receiver global unique identifier, and wherein the step of determining whether the encrypted package is valid comprises the steps of searching the client permissions database for a second receiver global unique identifier, and if not found, concluding that the package is invalid, and if found, comparing the receiver global unique identifier to the second receiver global unique identifier, determining whether they match, and if so, concluding that the package is valid, and if not, concluding that the package is invalid.

17. The method of claim 9 wherein the one or more permissions are selected from the group consisting of: an access count permission, an access time permission, an expiration date permission, an authorization date permission, a clipboard permission, a print permission, an unlimited access permission, an application permission, and a system-events permission.

18. The method of claim 9 wherein the computer executable file is password protected.

19. A system that communicates a package of information comprising:

a machine readable medium having information packaging software that generates a computer executable file comprising a package of information, the package of information comprising:

a file of data;

a permissions database having one or more permissions associated with the file of data;

an encryption software;

a network in communication with the machine readable medium;

a client computer system in communication with the network, the computer system adapted to receive the package of information and execute the computer executable file, the computer system having a client permissions database and a vault adapted to receive the package of information.

20. The system of claim 19 wherein the package of information further comprises a package global unique identifier, and the client computer system further comprises a module of computer code adapted to read the package global unique identifier, search the client permissions database for the package global unique identifier, and reject the package if the package global unique identifier is found in the client permissions database.

21. The system of claim 19 wherein the package of information further comprises a recipient global unique identifier, and the client computer system further comprises a module of computer code adapted to read the recipient global unique identifier, search the client permissions database for the recipient global unique identifier, and reject the package if the recipient global unique identifier is not found in the client permissions database.

22. The system of claim 19 wherein the one or more permissions are selected from the group consisting of: an access count permission, an access time permission, an expiration date permission, an authorization date permission, a clipboard permission, a print permission, an unlimited access permission, an application permission, and a system-events permission.

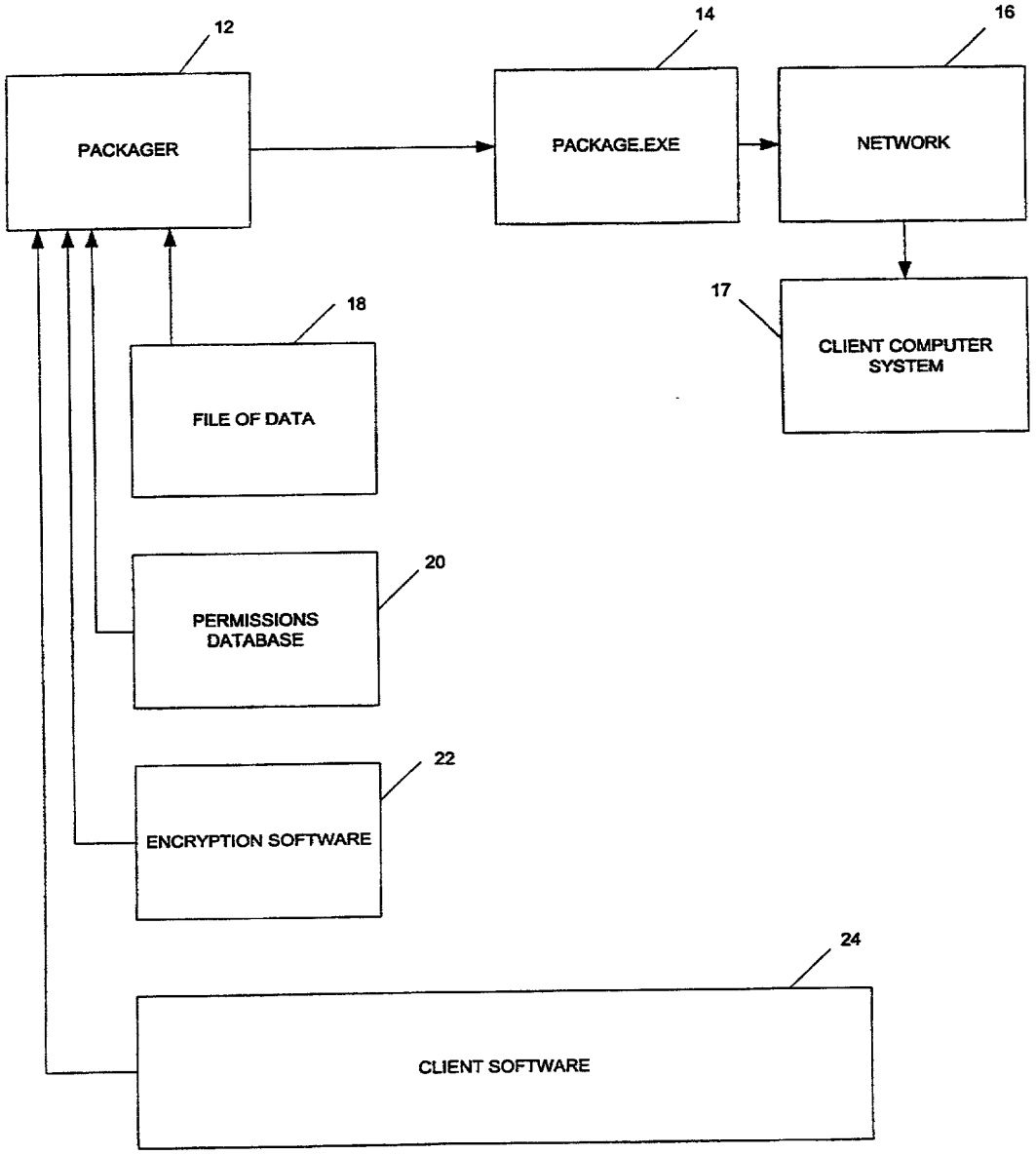
12
PACKAGER
14
PACKAGE.EXE
16
NETWORK
17
CLIENT COMPUTER SYSTEM
18
FILE OF DATA
20
PERMISSIONS DATABASE
22
ENCRYPTION SOFTWARE
24
CLIENT SOFTWARE

FIG. 1

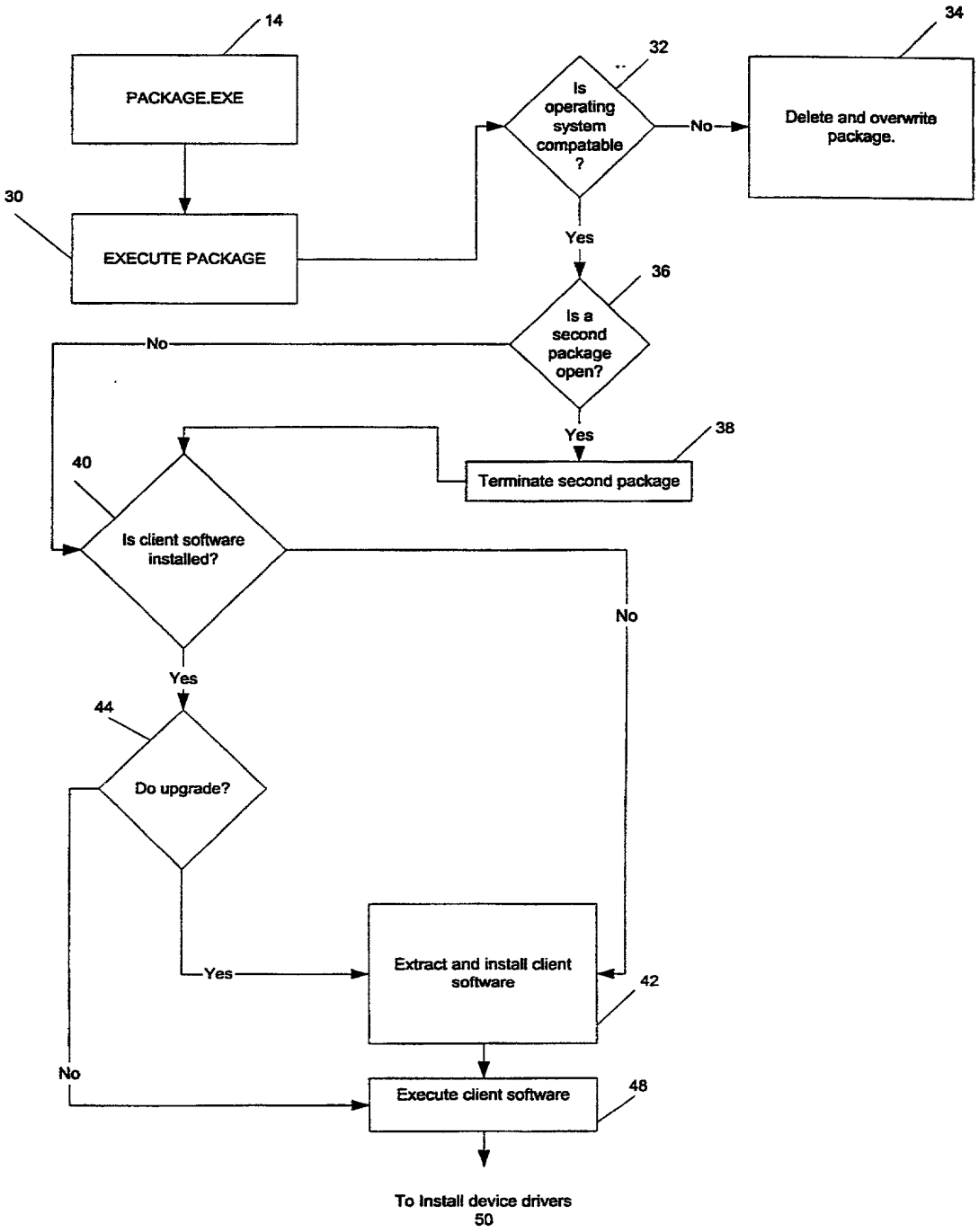
14
PACKAGE.EXE
30
EXECUTE PACKAGE
32
Is operating system compatable ?
No
34
Delete and overwrite package.
Yes
36
Is a second package open?
No
Yes
38
Terminate second package
40
Is client software installed?
No
Yes
44
Do upgrade?
Yes
Extract and install client software
42
No
Execute client software
48
To Install device drivers
50

FIG. 2a

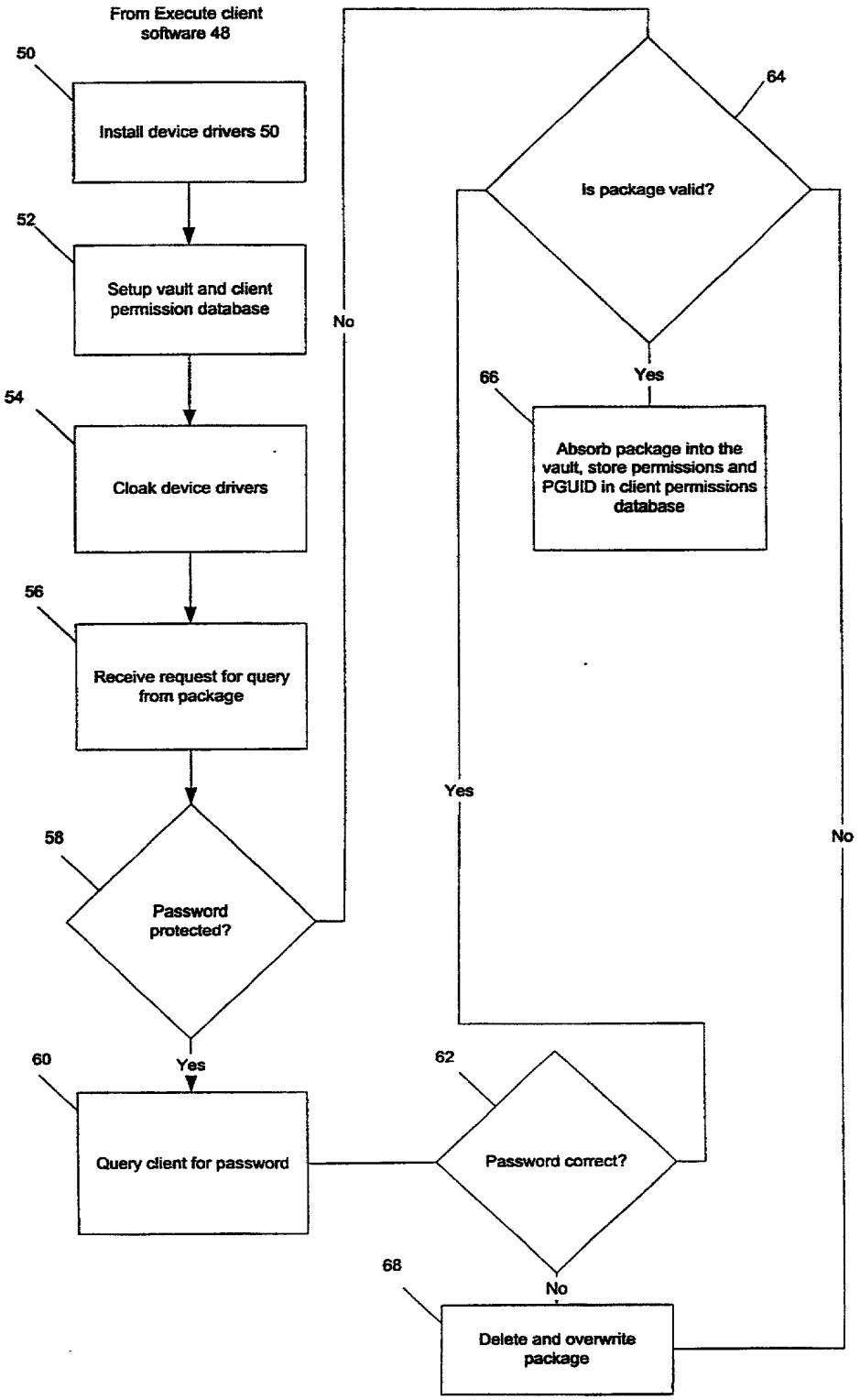
From Execute client software 48
50
Install device drivers 50
52
Setup vault and client permission database
54
Cloak device drivers
56
Receive request for query from package
58
Password protected?
No
Yes
60
Query client for password
62
Password correct?
No
Yes
64
Is package valid?
No
Yes
66
Absorb package into the vault, store permissions and PGUID in client permissions database
68
Delete and overwrite package

FIG. 2b

Doc. No. 1236-00

Declaration and Power of Attorney for Patent Application

As the below named inventor, we hereby declare that:

Our residence, post office address and citizenship are as stated next to our names,

We believe we are the original and first inventors of the subject matter which is claimed and for which a patent is sought on the invention entitled METHOD & APPARATUS FOR PACKAGING AND TRANSMITTING DATA the specification of which is filed herewith.

We hereby state that we have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

We acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, §1.56(a).

We hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before the application on which priority is claimed:

Prior Foreign Application(s)			Priority Claimed	
(Number)	(Country)	(Day/Month/Year Filed)	Yes	No

We hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §112, we acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of the application:

PCT/US00/26893	9/29/00	pending
(Application Serial No.)	(Filing Date)	(Status) (patent, pending, abandoned)

We hereby appoint the following attorneys and/or agents to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith:

T. Daniel Christenbury	Reg. No. 31,750
Guy T. Donatiello	Reg. No. 33,167
Paul A. Taufer	Reg. No. 35,703
Austin R. Miller	Reg. No. 16,602
James A. Drobile	Reg. No. 19,690
Gerard J. Weiser	Reg. No. 19,763
Robert A. McKinley	Reg. No. 43,793
Michael A. Patané	Reg. No. 42,982
Joan T. Kluger	Reg. No. 38,940
Sharon Fenick	Reg. No. 45,269
Stewart M. Wiener	Reg. No. 46,201
Armando A. Flores	Reg. No. 41,754
Felicity Rowe	Reg. No. 47,042

13

Address all telephone calls to Paul A. Taufer, Schnader Harrison Segal & Lewis LLP, Suite 3600, 1600 Market Street, Philadelphia, PA 19103 (215) 751-2475.

Address all correspondence to Paul A. Taufer, Schnader Harrison Segal & Lewis LLP, Suite 3600, 1600 Market Street, Philadelphia, PA 19103.

We hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under §1001 of Title 18 of the United States Code and that such wilful false statements may jeopardize the validity of the application or any patent issued thereon.

1-00

Full name of first and joint inventor: George Friedman

Inventor signature _____ TX

11/15/2000
Date

Residence: 7109 Montana Norte, Austin, Texas 78727
Citizenship: USA
Mailing Address: same as above

2-00

Full name of second and joint inventor: Robert Phillip Starek

Inventor signature Robert P. Starek

11/15/2000
Date

Residence: 1807 W. Slaughter Lane #200-482, Austin, Texas 78748
Citizenship: USA
Mailing Address: same as above

Full name of third and joint inventor: Carlos A. Murdock

Inventor signature _____ 11/15/2000
Date

Residence: 4517 Avenue F, Austin, Texas 78751
Citizenship: USA
Mailing Address: same as above